MOL2NET, International Conference Series on Multidisciplinary Sciences

Fatiguing Data to Protect against Cyber Security Extortions: A counter-intelligence methodology

Dr. Anthony Vincent B, Assistant Professor, Department of Computer Science
Kristu Jayanti College (Autonomous), Bangalore – 560024
anthonyvincent@kristujayanti.com

Graphical Abstract

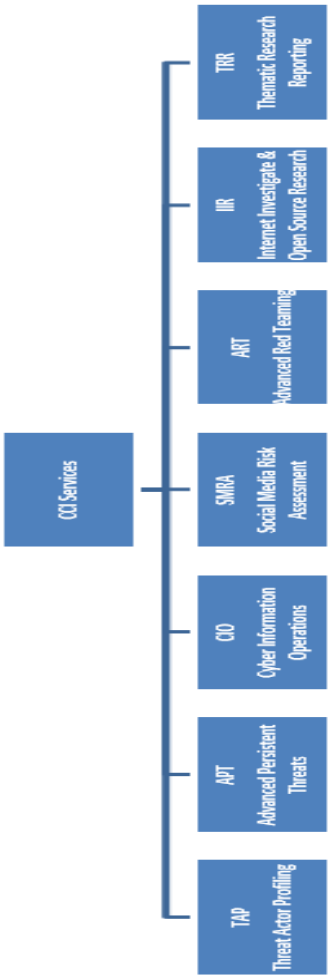

Figure 1: Counter Intelligence Services

Counter Intelligence Services:

1. Threat Actor Profiling (TAP) – understanding the 'who' of the five Ws (what, when, were, why) is a critical component of effectively assessing the threat that an opposing group presents to a company.

Abstract

"Now and recently, confab is less about preventing and stopping an attack, threat or exposure, and more about how swiftly you can detect that an attack is happening." There's a growing demand for security information and event management (SIEM) technologies and services, which gather and analyze security event big data that is used to manage threats. Big data offers the ability to analyze immense numbers of potential security events and make connections between them to create a prioritized list of threats. With big data, distinct data can be connected, which allows cyber security professionals to take a proactive approach that prevents attacks. Advanced Persistent Threats (APTs) are also used to find and identify where threats are coming from. Integrated security architecture and power of automated information collection and sharing between many security systems, called "Counter-intelligence" to solve the strategic short comings. "Counter intelligence" translates to new security product architecture into a data collection backbone feeding a centralized repository used to correlate security anomalies from, across multiple systems. This paper illustrates the new counter intelligence approach to defend against future cyber security threats by applying modern risk analysis and mitigation methods to protect users' private data from big data.

2. Advanced Persistent Threat (APT) – APT is an umbrella term used to describe the cyber portion of an on-going foreign intelligence gathering campaign; whereby increasingly sophisticated cyber threats seek to gain/maintain network access and collect intellectual property, personally identifiable information, and financial and/or strategic information from governments, corporations and *individuals.*

3. ***Cyber Information Operation (CIO)*** – CIO is a process of promoting a positive message about a Client over a negative messaging regarding a Client. Simply put the CIO service creates a greater positive narrative about the Client, than the negative narrative that is being created by other Internet users.

4. Social Media Risk Assessment (SMRA) – the ubiquity of social media in the work place has meant that it is becoming harder than ever for security teams to track employee social media use and the ways proprietary data may be flowing out of the Business..

5. Advanced Red Teaming Penetration Testing (ART) – we have the ability to simulate the threat of a range of cyber threat actors. From highly technical cyber espionage actors to the disruptive antics of 'script kiddy' activists, it has the ability to actively Penetration Test your infrastructure according to the threat posture of a large number of threat actor types.

6. Internet Investigation and Open Source Research and Analysis (IIR) – with the increasing spread of cyber space and the ubiquity of personal data on the Internet, for the wise researcher the Internet can prove to be a gold mine of valuable information for individuals with the skill and time to mine this source.

7. Thematic Research Reporting (TRR) – taking a deep dive look at strategic topics a TRR examines security issues that will affect a company over a protracted period of time.

Introduction

Cybercrime costs $118 billion annually and takes an average of 18 days to resolve at a cost of nearly $416,000 over those 18 days—and those figures are expected to grow as cyber-attacks continue to increase. Fortunately, tools and techniques now exist to handle the volume and complexity of today's cyber-attacks, enabling enterprises to stay ahead of evolving threats. [2] Combining big data analytics with security technologies yields a stronger defense posture. Big security analytics provide high-speed, automated analysis to bring network activity into clear focus to detect and stop threats, and shorten the time to remediation when attacks occur.

Conclusion

Big data will have an impact that will change most of the product categories in the field of computer security including solutions, network monitoring, authentication and authorization of users, identity management, fraud detection, and systems of governance, risk and compliance. Big data will change also the nature of the security controls as conventional firewalls, anti-malware and data loss prevention. In coming years, the tools of data analysis will evolve further to enable a number of advanced predictive capabilities and automated controls in real time. Our proposal of this paper is a turnkey solution provider for Cyber counter intelligence needs. Our research assessment process continuously monitors Cyber Threat developments and provide our customers with intelligence-based threat alerts and analysis. Working with industry leading cyber security partners, we are able to complement these alerts with solid technical consulting to countenance appropriate threat mitigation.

Future Enhancement

By 2019, more than 25% of global firms will adopt big data analytics for at least one security and fraud detection use case, up from current 8%. Big data analytics gives enterprises faster access to their own data than ever before. Big data analytics enables enterprises to combine and correlate external and internal information to see a bigger picture of threats against their enterprises. It is applicable in many security and fraud use cases such as detection of advanced threats, insider threats and account takeover. [3]

Organizations should align the capabilities security in a holistic cyber security strategy tailored to the threats and the risks specific to the demands of the organization, big data requires the collection of information from various sources and in different formats, a logical target is to have a single architecture to collect, index, normalize, analyse and share all the information, and organization should look for profile accounts, users or other entities, and look for anomalous transactions against those profiles. Organizations should ensure that the continued investment in security products promote technologies that use approaches agile-based analysis, not static signature-based tools to threats or on the edge of the network .Organizations are more than ever exposed to a large number and variety of threats and risks to cyber security. Big Data will be one of the main elements of change in the enterprises by supplying intelligence-driven models. Big data analytics will play a crucial role in detecting crime and security infractions in future cyber-space.

References

[1] Sean Bodmer, Gregory Carpenter, Lance James & David Dittrich , 2004, 'Hacking Back: Offensive Cyber Counterintelligence', Paperback, First Edition.

[2] Michael Minel, Michele Chambers & Ambiga Dhiraj, 2013, *'Big Data, Big Analytics: Emerging Business Intelligence and Analytic Trends for Today's Businesses'*, Wiley Publications, Hardcover.

[3] Frank J. Ohlhorst, 2013, 'Big Data Analytics: Turning Big Data into Big Money', Wiley & SAS Business Series.

[4 Big data: Cyber security's silver bullet. Available from <http://www.forbes.com/sites/kurtmarko/2014/11/09/big-data-cyber-security/>.[11 Sep 2014]

[5] CSC: Cyber Security Solutions <http://www.csc.com/cybersecurity/publications/>.[3 Mar 14]

[6] Terrogance Web Intelligence <http://www.terrogence.com/capabilities/cyber-counter-intelligence/>.[Since 2013]

[7] Big data cyber security Analytics in Action<http://www.drchaos.com/big-data-cyber-security-analytics-in-action/>.[25 Aug 2014]